

(19) 日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11) 特許出願公開番号

特開平11-231773

(43) 公開日 平成11年(1999) 8月27日

(51) Int.Cl.<sup>6</sup>

G 0 9 C 1/00

識別記号

6 1 0

F I

G 0 9 C 1/00

6 1 0 Z

審査請求 未請求 請求項の数 7 O L (全 7 頁)

(21) 出願番号 特願平10-28877

(22) 出願日 平成10年(1998) 2月10日

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 高橋 勝己

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

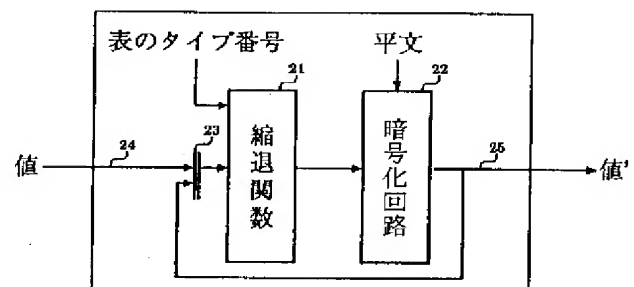
(74) 代理人 弁理士 高田 守 (外1名)

(54) 【発明の名称】 暗号強度評価装置

(57) 【要約】

【課題】 メッセージ長が同一で鍵長や暗号化手法の異なる暗号に対し同一構成の装置により評価可能にして、装置の規模や実行時間を短く抑える暗号強度評価装置を提供する。

【解決手段】 表を作成するために初期値を与える手段4と、初期値を変形して表の要素を生成する手段5と、生成した表を格納する手段7と、入手した暗号文を取り込む手段1、4、9と、暗号文を変形して表の要素と比較する手段11と、比較で一致したものが暗号文に対応する鍵であることを検証する手段12、13とからなり、前記暗号文を変形して表の要素と比較する手段は暗号文を変形して鍵を生成する鍵生成回路と、鍵を入力して暗号化する暗号化回路とを備えたL S I回路であり、L S I回路を交換することにより、メッセージ長が同一であれば、鍵長や暗号化手法の異なる暗号に対しても同一構成の装置により暗号を評価可能にした。



## 【特許請求の範囲】

【請求項1】 平文を設定し、複数の表を作成するために初期値を与える手段と、初期値を変形して表の要素を生成する手段と、生成した表の要素を格納する手段と、入手した暗号文を取り込む手段と、表を取りだし暗号文を変形させて表の要素と比較する作業を繰り返す手段と、比較の結果一致したものが暗号文に対応する鍵であることを検証する手段とからなり、予め平文を想定して大量の表を作成し、暗号文入手後、その暗号文の加工と前記表との比較を繰り返しながら、暗号文の鍵を求めることを特徴とする暗号強度評価装置。

【請求項2】 前記暗号文を変形させて表の要素と比較する作業を繰り返す手段は暗号文を入力して変形し鍵を生成する鍵生成回路と、前記鍵及び平文を入力して暗号化を行なう暗号化回路とを有するLSI回路からなることを特徴とする請求項1記載の暗号強度評価装置。

【請求項3】 前記暗号文を変形し鍵を生成する鍵生成回路を他の鍵長の鍵を生成する鍵生成回路に交換することにより、メッセージ長が同じで鍵長の異なる暗号を評価するようにしたことを特徴とする請求項2記載の暗号強度評価装置。

【請求項4】 前記鍵を入力して暗号化を行なう暗号化回路を他の暗号を行なう暗号化回路に交換することにより、メッセージ長が同一の他の暗号を評価するようにしたことを特徴とする請求項2または3記載の暗号強度評価装置。

【請求項5】 前記暗号文を変形し鍵を生成する鍵生成回路を他の鍵長の鍵の一部を変数として外部から受けとる回路に交換することにより、メッセージ長が同じで、鍵長がメッセージ長を越える他の暗号を評価するようにしたことを特徴とする請求項2記載の暗号強度評価装置。

【請求項6】 前記暗号文を変形し、鍵を生成する鍵生成回路に拡大転置を採用することによって、メッセージ長が同じで、鍵長がメッセージ長を越える他の暗号を評価するようにしたことを特徴とする請求項2記載の暗号強度評価装置。

【請求項7】 前記平文を入力して暗号化を行なう暗号化回路を複数設け、前記複数の暗号化回路のそれぞれに異なる平文を入力して暗号化し、前記鍵生成回路にその複数の暗号文を入力して鍵を生成するようにしたことにより、メッセージ長が同じで、鍵長がメッセージ長を越える他の暗号を評価するようにしたことを特徴とする請求項2記載の暗号強度評価装置。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、予め平文を想定し、暗号文に対応する鍵を探索することで暗号の強度を評価する暗号強度評価装置に関する。

## 【0002】

【従来の技術】予め表を作成し、暗号文を加工しつつ表との比較を繰り返す暗号強度評価は、『M.E.Hellman, "A cryptanalytic time-memory trade-off", IEEE Transaction on Information Theory, Vol.IT-26 No.4』という論文に述べられている。ここで、暗号の強度とは、暗号を解くために要するコスト（例えば、装置の大きさや解読時間など）であり、従って、暗号強度を評価するということは、暗号解読の結果そのコストを評価することになる。

## 【0003】

【発明が解決しようとする課題】しかしながら、この論文では暗号強度評価の手法が述べられているだけであり、この装置を構成する方法、すなわち、この手法を実現した装置または実現する手段については述べられていない。

【0004】本発明は、上記従来の問題を解決するためになされたもので、上記論文に基づく手法を実現するための手段を提供し、特にメッセージ長が同一であり、鍵長や暗号化手法の異なる暗号に対し同一構成の装置により評価可能にして、装置の規模や実行時間を短く抑えるようにした暗号強度評価装置を提供することを目的とする。

## 【0005】

【課題を解決するための手段】請求項1にかかる発明における暗号強度評価装置は、平文を設定し、複数の表を作成するために初期値を与える手段と、初期値を変形して表の要素を生成する手段と、生成した表の要素を格納する手段と、入手した暗号文を取り込む手段と、表を取りだし暗号文を変形させて表の要素と比較する作業を繰り返す手段と、比較の結果一致したものが暗号文に対応する鍵であることを検証する手段とからなり、予め平文を想定して大量の表を作成し、暗号文入手後、その暗号文の加工と前記表との比較を繰り返しながら、暗号文の鍵を求めるようにしたものである。

【0006】請求項2にかかる発明における暗号強度評価装置は、前記暗号文を変形させて表の要素と比較する作業を繰り返す手段は暗号文を入力して変形し鍵を生成する鍵生成回路と、前記鍵及び平文を入力して暗号化を行なう暗号化回路とを有するLSI回路からなるようにしたものである。

【0007】請求項3にかかる発明における暗号強度評価装置は、前記暗号文を変形し鍵を生成する鍵生成回路を他の鍵長の鍵を生成する鍵生成回路に交換することにより、メッセージ長が同じで鍵長の異なる暗号を評価するようにしたものである。

【0008】請求項4にかかる発明における暗号強度評価装置は、前記鍵を入力して暗号化を行なう暗号化回路を他の暗号を行なう暗号化回路に交換することにより、メッセージ長が同一の他の暗号を評価するようにしたものである。

【0009】請求項5にかかる発明における暗号強度評価装置は、前記暗号文を変形し鍵を生成する鍵生成回路を他の鍵長の鍵の一部を変数として外部から受け取る回路に交換することにより、メッセージ長が同じで、鍵長がメッセージ長を越える他の暗号を評価するようにしたものである。

【0010】請求項6にかかる発明における暗号強度評価装置は、前記暗号文を変形し鍵を生成する鍵生成回路に拡大転置を採用することによって、メッセージ長が同じで、鍵長がメッセージ長を越える他の暗号を評価する

ようにしたものである。  
【0011】請求項7にかかる発明における暗号強度評価装置は、前記平文を入力して暗号化を行なう暗号化回路を複数設け、前記複数の暗号化回路のそれぞれに異なる平文を入力して暗号化し、前記鍵生成回路にその複数の暗号文を入力して鍵を生成するようにしたことにより、メッセージ長が同じで、鍵長がメッセージ長を越える他の暗号を評価するようにしたものである。

【0012】

【発明の実施の形態】以下、添付図面、図1乃至図3に基づき、本発明の一実施の形態を詳細に説明する。図1は本発明の一実施の形態における暗号強度評価装置の構成を示すブロック図、図2は図1に示す暗号強度評価装置において暗号化の処理を行なうLSIの詳細を示す構成図、図3は図2に示す暗号化回路を複数設けたLSIの詳細を示す構成図である。

【0013】実施の形態1. まず、図1を参照して、本発明の実施の形態における暗号強度評価装置の構成を説明する。以下、本実施の形態では、DESという暗号を例に用いて説明する。DESは、鍵長56ビット、メッセージ長(平文や暗号文の長さ)64ビットとする暗号である。

【0014】図1において、1は装置全体の管理やユーザとのインターフェイスを担うローカルコンピュータ、2a、2bはローカルコンピュータ1からの指示で処理を行なうそれぞれ一纏めにまとめたユニットであり、3はローカルコンピュータ1と各ユニット2a、2bとの間でデータの送受信を行なうためのネットワーク、4はユニット2a、2b内全体を管理する制御用プロセッサであり、内部にローカルメモリーを有する。

【0015】また、5a、5bは事前処理(暗号文作成のための表を作成する処理)において、初期値から暗号解読のための表の要素を作成する処理(暗号化処理、後述する)を行なうLSI、6はデータを送受信のためのバス、7は表などを蓄える記憶装置、8a、8bは解読処理において値の検索を行なう検索ブロック、9は表の要素の検索を制御するプロセッサ、10は表などを展開するメモリー、11は暗号文を加工し変形させる(暗号化処理、後述する)ためのLSIであり、検索ブロック8a、8bはこれらプロセッサ9、メモリー10、L

SI11から構成される。12は検索ブロックが求めた解の候補を検証する検証用プロセッサであり、13は検証用プロセッサ12が検証する際に、値を加工する(暗号化処理、後述する)LSIである。

【0016】尚、本実施の形態において、制御用プロセッサ4により平文を設定し、複数の表を作成するために初期値を与える手段を構成し、LSI5a、5bにより初期値を変形して表の要素を生成する手段を構成し、記憶装置7により生成した表の要素を格納する手段を構成し、ローカルコンピュータ1、制御用プロセッサ4、プロセッサ9により入手した暗号文を取り込む手段を構成し、LSI11により表を取りだし暗号文を変形させて表の要素と比較する作業を繰り返す手段を構成し、検証用プロセッサ12及びLSI13により比較の結果一致したものが暗号文に対応する鍵であることを検証する手段を構成する。

【0017】次に、図2を参照して、図1に示す暗号強度評価装置において暗号化の処理を行なうLSIの詳細な構成を説明する。すなわち、図2に示すLSIは、基本的には、図1に示すLSI5、22、23の全てに適用されるものである。しかし、違いとしては、LSIを使用している部所の役割りに応じて暗号化処理の反復回数が異なるよう動作することである。

【0018】図2において、21は縮退関数によって暗号文を変形し鍵を生成する鍵生成回路としての縮退関数回路(単に、縮退関数ともいう)、22は縮退関数21で変形された値を鍵として暗号化を行なう暗号化の回路または暗号化回路、23は64ビットの2入力1出力のセレクタである。セレクタ23は外部からの初期値と内部でループする際の値を切替える。24は縮退関数21に対して入力する64ビットのデータ線、25は暗号化回路22から出力する64ビットのデータ線である。

【0019】次に、図1及び図2を参照して、本発明の実施の形態における暗号強度評価装置の動作を説明する。本実施の形態における動作を、暗号文入手前にその解読のための表を作成する事前処理と、暗号文入手後にその表を用いて解読する解読処理及び解読の結果を評価する評価処理(評価処理を解読処理に含めて解読処理ともいう)との2つに分けて説明する。また、ここでいう事前処理は暗号解読のための表を作成して記憶手段に格納する処理をいう。

【0020】まず、事前処理は次のような処理手順で行なわれる。

(1) ローカルコンピュータ1は、ユーザの指示に従い平文などの処理に必要なパラメータを決定する。

【0021】(2) ローカルコンピュータ1は、表作成の処理を各ユニット2a、2bに分配する。この時、ローカルコンピュータ1は、ネットワーク3を介し、平文、作成する表のタイプ(表タイプ番号100番から200番など)、表の要素数M及び表作成のための加工繰り返

し数T等をパラメータとして各ユニット2a、2b内の制御用プロセッサ4へ送る。

【0022】(3) 制御用プロセッサ4は、平文、表のタイプ、初期値及び加工繰返し回数T等といったパラメータをLSI5a、5bへ送り、表の要素の作成を指示する。この時、初期値は、表のタイプと作成する要素の表での指標値（インデックス(index) 番号）から生成する。例えば、その初期値の値は、『表のタイプ番号  $\ll \log(M) + \text{指標値}$ 』で作成することができる。

【0023】(4) 各LSI5a、5bは、平文と初期値を入力として、指定された表のタイプに応じた処理を行ない新しい値を生成する。LSI5a、5bは内部ループを持ち、この値を初期値の代わりに用いて、更に新しい値を生成するこれをT回数繰返す。この後、各LSI5a、5bは要素作成が終了した後、制御用プロセッサ4にその終了報告を行なう。

【0024】(5) 制御用プロセッサ4は、終了報告を受けとった後、作成した値をLSI5a、5bから取りだし、次の表の要素作成を各LSI5a、5bに指示する。この指示は、制御用プロセッサ4の処理が終了するまで繰返される。

【0025】(6) 制御用プロセッサ4は、表の全ての要素を受けとると、バス6を介して、その表を記憶装置7に書き込む。この時、表の各要素から、その作成に用いられた初期値を求めるのに必要な情報も合わせて格納する。これを全ての表を作成するまで繰返す。

【0026】(7) 制御用プロセッサ4は、全ての表の作成が終了すると、その旨をローカルコンピュータ1に報告する。

(8) ローカルコンピュータ1は、全てのユニット2a、2bから終了報告を受けとるまで待つ。以上の動作で、事前処理は終了する。

【0027】次に、解読処理は次のような処理手順で行なわれる。

(1) ローカルコンピュータ1に暗号文が入力される。  
(2) ローカルコンピュータ1は、暗号文をネットワーク3を介して各ユニット2a、2bの制御用プロセッサ4へ送る。

【0028】(3) 制御用プロセッサ4は、暗号文を検索ブロック8a、8bの全てに送った後、記憶装置7から表を取り出して各検索ブロック8a、8bに配布する。

(4) 検索ブロック8a、8bのプロセッサ9は、暗号文と表を受けとると、それをメモリー10に格納する。

【0029】(5) プロセッサ9は、入手した暗号文と表の各要素（暗号化したもの）との比較を行なう。比較した際、表の要素の中に一致するもの（解読したことになる）があれば、その要素の指標から、その要素が生成される際に用いられた初期値を求める。

【0030】(6) (5) で表の要素と一致しなかった場合、プロセッサ9は、LSI11に対し暗号文を入力し

て処理させ、表から新しい値を取り出して、更に表の各要素との比較を行なう。表の要素の中に一致するものがあれば、その要素の指標から、その要素が生成される際に用いられた初期値を求める。一致するものがあつた場合には、下記(17)の処理に移る。

【0031】(7) プロセッサ9は、(6) 項における比較結果の如何に拘らず、LSI11が処理してできた新しい値を入力として更に処理させ、それによってできた新しい値を取り出して、表の各要素との比較を行なう。表の要素の中に一致するものがあつた場合には、その要素の指標から、その要素が生成される際に用いられた初期値を求める。

【0032】(8) 事前処理において加工を繰返し行なった回数Tだけ(7) 項の処理を繰返す。

(9) プロセッサ9は、(6) ~ (8) 項の処理結果について一致した値の有無と、一致した場合の対応する初期値と、それが (6) の処理を1回目として何回目の加工だったかという情報とを制御用プロセッサ4に報告する。

【0033】(10) 制御用プロセッサ4は、一致した値が報告された場合、その初期値、検索における加工回数、平文、表のタイプ番号及び表作成時の加工回数Tを検証用プロセッサ12に送る。また、制御用プロセッサ4は、一致した値の有無に拘らず、記憶装置7から他の表を取り出し、ブロック8a、8bに同様の処理を指示する。この作業は、全ての表に対する処理が終了するまで繰返される。

【0034】(11) 検証用プロセッサ12は、表作成時に行なわれた加工回数Tから比較処理で一致するまでに、LSI11が処理した回数を引いた値を求め、この値、初期値、平文及び表のタイプ番号をLSI13に送る。

【0035】(12) LSI13は、上記(11) 項で減算した値と、初期値、平文及び表のタイプ番号とを受けとり、指定した回数、及び、その回数よりも1回少ない回数処理した結果（暗号の解読結果である鍵を生成するために必要）の2つを検証用プロセッサ12に送る。

【0036】(13) 検証用プロセッサ12は、LSI13から受けとった値のうち、指定した回数処理した結果を入手した暗号文と比較する。ここで、値が一致した場合は、1回分処理の少ない値を入力して縮退関数の値を求め、それを解読結果（鍵）だとして、制御用プロセッサ4に報告する。

【0037】(14) 制御用プロセッサ4は、解読結果を受けとった場合、ネットワーク3を介してその値をローカルコンピュータ1に報告する。一方、終了報告を受けとった場合には、他の検証すべき値を検証用プロセッサ12に送る。

【0038】(15) 制御用プロセッサ4は全ての表の処理が終了した場合、ローカルコンピュータ1に対して、その終了報告を行なう。

(16) ローカルコンピュータ1は、解読結果(鍵)を受けとった場合、その値を表示すると共に、各ユニット2a、2bに対し処理の中止を指示する。また、解読結果を受けとらず、全てのユニット2a、2bから終了報告を受けとった場合、鍵が発見できなかった旨を表示する。

【0039】(17) 制御用プロセッサ4は、(5)において一致した値が報告された場合、表作成時の加工回数Tから1を引いた値、一致した要素に対応する初期値、平文及び表のタイプ番号を検証用プロセッサ12に送る。検証用プロセッサ12は、これらの値をLSI13に転送する。LSI13は、初期値、平文及び表のタイプ番号を受けとり、その処理を指定されたT-1回繰り返す。検証用プロセッサ12は、LSI13から処理結果の値を受けとり、この値を縮退関数の引数として関数の値を求め、これを解読結果(鍵)だとして制御用プロセッサ4に報告する。制御用プロセッサ4は、解読結果を受けとった場合、その値をローカルコンピュータ1にネットワーク3を介して報告する。ローカルコンピュータ1は、解読結果(鍵)を受けとった場合、その値を表示すると共に、各ユニット2a、2bに対し処理の中止を指示する。以上で、解読処理動作を終了する。

【0040】実施の形態2. 以下、図2を参照して、実施の形態2、3、4及び5における暗号化の処理について説明する。暗号化回路22は、56ビットの鍵を要求するため、縮退関数21は入力した暗号文64ビットから54ビットへの変換とその値の変形とを実行する。暗号化回路22が56ビットを越える鍵を要求する場合は、取り除くビット数を減らした縮退関数(鍵生成回路)に交換する、すなわち、LSIを交換することによって、鍵長の異なる暗号に対応させることができるようにした。

【0041】実施の形態3. 実施の形態2においては、図2に示す暗号化回路22は、DESの暗号化を行なうようにしたが、実施の形態3においては、これを他の暗号化回路に変える、すなわち、LSIを交換することによって、異なる暗号(例えば、DES、FEEL)に対応することができるようにした。

【0042】実施の形態4. 実施の形態2においては、図2に示す縮退関数21は、ビット数の削減とその値の変換とを行なうものとした。そのため、縮退関数21は、メッセージ長を越える鍵長を生成することができなかった。しかし、鍵長がメッセージ長を越える場合、暗号文を変形し鍵を生成する回路を他の鍵長の鍵の一部を変数として外部から受けとる回路に交換して、別途外部から値を取り込むようにすることによって、メッセージ長を越える鍵長に対応させることができる。この外部から取り込む値は、装置の利用者もしくは装置自体が定数として与える方法がある。また、表の初期値と同様に、表の要素番号、表のタイプ番号及び縮退関数と、暗号化

を繰り返した回数等といった値を引数とした関数値を与える方法もある。この関数値としてもっとも簡単なものは、引数をそのまま関数値として返す関数である。すなわち、このように、LSIを交換することによって、メッセージ長ビット以上の鍵長のものに対応するようにした。

【0043】尚、メッセージ長の方が大きい場合には、1つの暗号文だけでは、鍵を特定することはできない。このため、もう1つ別の平文とその暗号化の結果である暗号文が必要になる。この場合、2つの平文に対し、生成した2つ暗号文が、両方とも、入手した2つの暗号文と一致した場合にのみ、それが鍵であると見做される。

【0044】実施の形態5. 実施の形態4においては、鍵長がメッセージ長を越える場合、不足分を開部からの入力で賄うようにしたが、DESの内部処理で行なっているような、暗号文を変形し鍵を生成する回路に拡大転置を用いてビット長を増やす方法がある。このように、LSIを交換することによって、メッセージ長ビット以上の鍵長のものに対応するようにした。尚、拡大とはビット数を増やすこと、転置とはビットを入れ換えることである。

【0045】実施の形態6. 次に、図3を参照して、複数の平文を用いて暗号化を処理するLSIについて説明する。実施の形態4及び5においては、平文を1つとして処理を行なうようにしたが、本実施の形態では、その平文を複数に増やすことによって不足分を補う方法を採用する。

【0046】図3において、31は縮退関数によって暗号文を変形し鍵を生成する鍵生成回路としての縮退関数回路(単に、縮退関数ともいう)、32は縮退関数31で変形された値を鍵として暗号化を行なう暗号化回路、33はセレクトである。すなわち、図3は、図2の暗号化回路を複数にしたものである。

【0047】次に、図3を参照して、複数の平文を用いて暗号化を処理するLSIの動作について説明する。縮退関数31は、セレクト33の値と線36の値を受けとり、鍵を生成する。セレクト33が線34の値を選択する場合、暗号化回路32bの出力である線36の値は予め設定した値となる。ここで設定する値は通常0である。

【0048】すなわち、本実施の形態においては、鍵長がメッセージ長を越える場合、複数の異なる平文を用意し、暗号文を変形し鍵を生成する回路に複数の暗号文を入力として与え、鍵を生成するよう、LSIを交換することによって、メッセージ長ビット以上の鍵長のものに対応するようにした。

【0049】以上説明した図1乃至図3に示す回路はハードウェアにより実現されるが、ソフトウェアによって実現することも可能である。

【0050】

【発明の効果】請求項1及び2にかかる発明は、上記のように構成し、特に処理の入出力をメッセージ長に合わせ、メッセージ長が同一であれば、LSIを交換するだけで同一構成の装置により、異なる鍵長または異なる暗号化手法に容易に対応して評価可能にしたことにより、暗号強度評価装置の規模や実行時間を短く抑えることができる暗号強度評価装置を提供することができる。

【0051】請求項3にかかる発明は、上記のように構成し、特にLSIを交換して鍵生成回路を変えることにより、メッセージ長ビット以下の鍵長の違うものに対応

【0052】請求項4にかかる発明は、上記のように構成し、特にLSIを交換して暗号化回路を異なる暗号のものに変えることにより、メッセージ長が同じ他の暗号に対応することができる。

【0053】請求項5にかかる発明は、上記のように構成し、特にLSIを交換して、暗号文を変形し鍵を生成する回路を他の鍵長の鍵の一部を変数として外部から受けとる回路にかえることにより、メッセージ長ビット以上の鍵長のものに対応することができる。

【0054】請求項6にかかる発明は、上記のように構成し、特にLSIを交換して、暗号文を変形し鍵を生成する回路に拡大転置を採用することにより、メッセージ長ビット以上の鍵長のものに対応することができる。

【0055】請求項7にかかる発明は、上記のように構成し、特にLSIを交換して、複数の異なる平文をそれぞれ入力して暗号化し、その複数の暗号文を入力して鍵を生成することにより、メッセージ長ビット以上の鍵長のものに対応することができる。

#### 【図面の簡単な説明】

【図1】 本発明の一実施の形態における暗号強度評価装置の構成を示すブロック図、

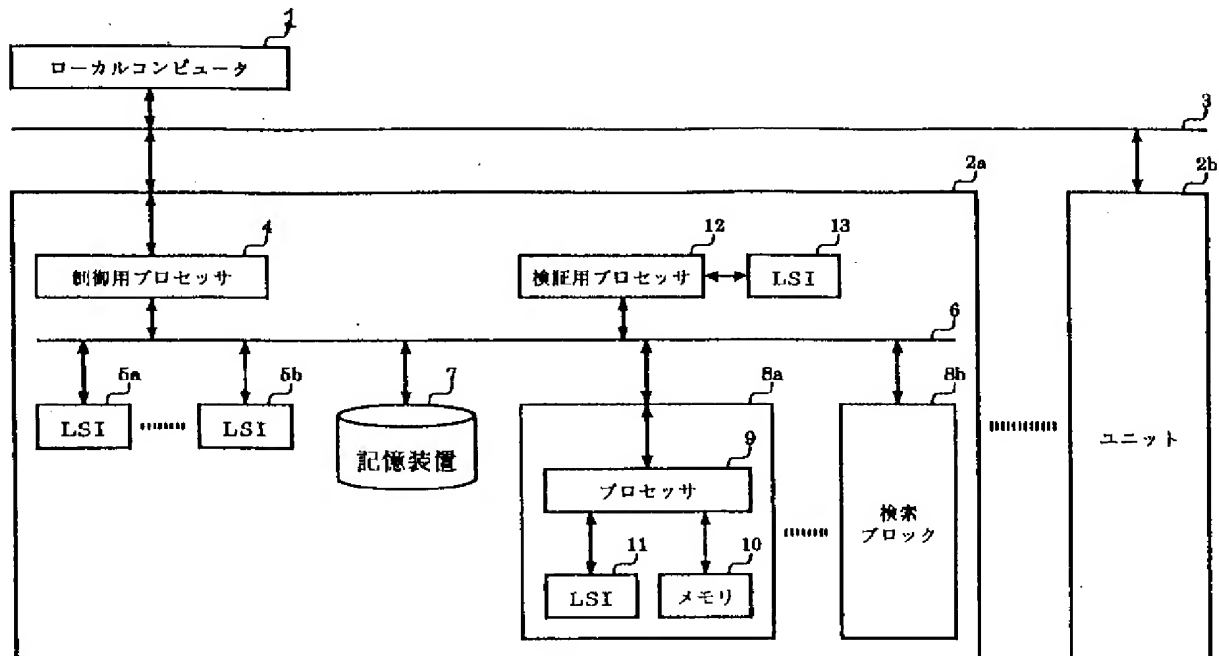
【図2】 図1に示す暗号強度評価装置において暗号化の処理を行なうLSIの詳細を示す構成図、

【図3】 図2に示す暗号化回路を複数設けたLSIの構成を詳細に示す図である。

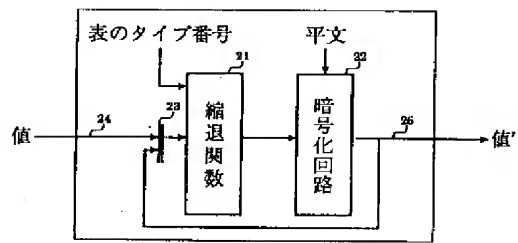
#### 【符号の説明】

1 ローカルコンピュータ、 2a、2b ユニット、  
3 ネットワーク、4 制御用プロセッサ、 5a、  
5b 事前処理用LSI、 7 記憶装置、6 バス、  
8a、8b 検索ブロック、 12 検証用プロセッサ、  
9 検索用プロセッサ、 10 メモリ、 32a、32b  
縮退関数回路、11 解読処理における検  
索用LSI、 13 解読処理における検証用LSI  
21 暗号化回路、 22 縮退関数回路、 24、25  
外部との入出、23 セレクタ、 31 暗号化回  
路、 33 セレクタ、34、35 外部との入出力  
線、 36 暗号化回路32bの出力線。

【図1】



【図2】



【図3】

